INTERNATIONAL STANDARD

ISO/IEC 19823-19

First edition
2018-09

Information technology — Conformance test methods for security service crypto suites —

Part 19: Crypto suite RAMON

Technologies de l'information — Méthodes d'essai de conformité pour les suites cryptographiques des services de sécurité —

Partie 19: Suite cryptographique RAMON

Reference number
ISO/IEC 19823-19:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

A list of all parts in the ISO 19823 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

ISO/IEC 29167 describes security as applicable for ISO/IEC 18000. The various parts of ISO/IEC 29167 describe crypto suites that are optional extensions to the ISO/IEC 18000 air interfaces.

ISO/IEC 19823 describes the conformance test methods for security service crypto suites. ISO/IEC 19823 is related to ISO/IEC 18047, which describes the radio frequency identification device conformance test methods, in the same way as ISO/IEC 29167 is related to ISO/IEC 18000.

These relations mean that, for a product that is claimed to be compliant to a pair of ISO/IEC 18000-n and ISO/IEC 29167-m, the test methods of ISO/IEC 18047-n and ISO/IEC 19823-m apply. If a product supports more than one part of ISO/IEC 18000 or ISO/IEC 29167, all related parts of ISO/IEC 18047 and ISO/IEC 19823 apply.

NOTE The conformance test requirements of ISO/IEC 18000-6, ISO/IEC 18000-61, ISO/IEC 18000-62, ISO/IEC 18000-63, ISO/IEC 18000-64 are currently all in ISO/IEC 18047-6.

This document describes the test methods for the RAMON crypto suite as standardized in ISO/IEC 29167-19.

NOTE Test methods for interrogator and tag performance are covered by ISO/IEC 18046 (all parts).

Information technology — Conformance test methods for security service crypto suites —

Part 19: Crypto suite RAMON

1 Scope

This document describes test methods for determining the conformance of security crypto suites with the specifications given in ISO/IEC 29167-19.

This document contains conformance tests for all mandatory and optional functions.

The conformance parameters are the following:

— parameters that apply directly, affecting system functionality and inter-operability;

— protocol including commands and replies;

— nominal values and tolerances.

Unless otherwise specified, the tests in this document are exclusively applicable in relation to RFID tags and interrogators defined in the ISO/IEC 18000 series using a reference to this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 18000-63:2015, *Information technology — Radio frequency identification for item management — Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C*

ISO/IEC 18047-6:2017, *Information technology — Radio frequency identification device conformance test methods — Part 6: Test methods for air interface communications at 860 MHz to 960 MHz*

ISO/IEC 19762, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

ISO/IEC 29167-19:2016, *Information technology — Automatic identification and data capture techniques — Part 19: Crypto suite RAMON security services for air interface communications*

3 Terms, definitions, symbols and abbreviated terms

For the purposes of this document, the terms and definitions, symbols and abbreviated terms given in ISO/IEC 19762 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

4 Test methods

4.1 General

Clause 4 describes the general test methods for ISO/IEC 29167-19. As the parts of ISO/IEC 19823 are always tested in relation to ISO/IEC 18047, a duplication of information requirements and specifications should be avoided.

Clause 5 defines elements that are assumed to be covered in the respective ISO/IEC 18047 part and therefore shall not be addressed in an ISO/IEC 19823 part. They may only be defined in ISO/IEC 19823 if ISO/IEC 18047 does not define them, although a revision of ISO/IEC 18047 should be the preferred option.

Clause 6 defines elements that are not expected to be covered by ISO/IEC 18047 and therefore shall be addressed in the respective ISO/IEC 19823 part.

4.2 By demonstration

Laboratory testing of one, or (if required for statistical reasons) multiple, products, processes or services to ensure conformance. A laboratory shall perform the indicated testing to ensure conformance of the component or system.

For Protocol requirements that are verified **by demonstration**, the test conditions are specified by this document. The detailed test plan is at the discretion of the laboratory.

4.3 By design

Design parameters and/or theoretical analysis that ensure conformance. A vendor submitting a component or system for conformance testing shall provide the necessary technical information, in the form of a technical memorandum or similar. A laboratory shall approve the technical analysis as being sufficient to ensure conformance of the component or system.

For Protocol requirements that are verified **by design**, the method of technical analysis is at the discretion of the submitting vendor and is not specified by this document. In general, the technical analysis shall have sufficient rigor and technical depth to convince a test engineer knowledgeable of the Protocol that the particular requirement has been met.

5 Test methods with respect to ISO/IEC 18000 parts

5.1 Test requirements for ISO/IEC 18000-63 interrogators and tags

Interrogators and tags tested according this document shall be based on ISO/IEC 18000-63. Test requirements for ISO/IEC 18000-63 interrogators and tags shall be as specified in ISO/IEC 18047-6:2017, Clauses 4 and 5.

Before a DUT is tested according to this document, it shall meet the requirements of ISO/IEC 18047-6:2017, Clause 8.

5.2 Test requirements for other parts of ISO/IEC 18000

Currently there are no test methods defined for other parts of ISO/IEC 18000.

6 Test methods with respect to ISO/IEC 29167-19 interrogators and tags

6.1 Test map for optional features

Interrogators and tags tested according this document shall be based on ISO/IEC 29167-19. Table 1 lists all optional features of this crypto suite and shall be used as a template to report the test results. Furthermore, it is used to refer to the test requirements in Table 2.

Table 1 — Test map for optional features

#	Feature	Additional requirement	Mark items to be tested for supplied product	Test results
1	Mutual authentication	Shall be tested with the authenticate command of the declared ISO/IEC 18000 part		
2	Secure communication	Shall be tested with the authenticate command of the declared ISO/IEC 18000 part		
3	Key update	Shall be tested with the authenticate command of the declared ISO/IEC 18000 part		
4	Number of keys supported			
5	Key length supported by the tag			

Table 2 lists all crypto suite requirements that shall be tested in dependence of the features of Table 1 as supported by the DUT.

6.2 Crypto suite requirements

Table 2 — Crypto suite requirements

Item	Protocol subclause[a]	Requirement[a,b]	M/O/ PRM/CRM[c]	Applies to	How to verify
1	6.2.1	The Interrogator shall compare its generated Interrogator challenge with the challenge it received from the Tag. If the values match, the Tag is identified.	M	Interrogator	By demonstration using Test Pattern 12 and Test Pattern 14
2	6.2.1	If the Tag provides a signature along with the SID, the Interrogator shall validate the signature using the signature verification key. If successful, the Tag is authenticated.	M	Interrogator	By design
3	6.5	The IID shall remain constant during a session.	M	Interrogator	By design
4	6.5	The SID of a Tag shall be set during personalization and shall remain constant throughout the lifetime of the Tag.	M	Tag	By design
5	6.5	The SID and the optional signature are secret information and shall never be readable for an unauthorized reader.	M	Tag	By design
6	6.5	The SID shall never be sent in plaintext.	M	Tag	By design

Table 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a,b]	M/O/ PRM/CRM[c]	Applies to	How to verify
7	6.5	The Tag shall not perform signature generation or verification, nor shall it store the corresponding keys.	M	Tag	By design
8	6.5	The Tag shall store the SID and the public key K_E for Tag authentication in its memory.	M	Tag	By design
9	6.5	The Tag shall store the SID along with its signature in its memory.	O	Tag	By design
10	6.5	The memory locations storing the SID and the secret keys shall not be readable for any Interrogator after having written these values once during production of the Tag.	M	Tag	By design
11	6.5	The Interrogator shall have access to the RAMON decryption key K_D to be able to decrypt the authentication message sent by the Tag.	M	Interrogator	By design
12	6.5	The Interrogator shall have access to a list of valid SIDs; each SID might have a signature attached to it.	M	Interrogator	By design
13	6.6	The length of the keys used for Tag identification shall be as specified in Table 4.	M	Tag, Interrogator	By design
14	6.6	The length of the keys used for mutual authentication and secure communication shall be as specified in Table 5.	M	Tag, Interrogator	By design
15	8.1	A Tag shall support at least one of two authentication protocol modes, the partial result mode or the complete result mode.	M	Tag	By design
16	8.1	Interrogators shall support both protocol modes.	M	Interrogator	By demonstration using Test Pattern 12 and 13
17	8.1	The complete result mode shall require the capability of the interface standard to handle long timeouts or to signalize the interrogator that a tag is still processing a command.	M	Interrogator, Tag	By design
18	8.1	In partial result mode, a sequence of Authenticate commands shall be sent to the Tag in order to complete the full authentication protocol.	M	Interrogator, Tag	By design

Table 2 *(continued)*

Item	Protocol subclause[a]	Requirement[a,b]	M/O/ PRM/CRM[c]	Applies to	How to verify
19	8.1	A Tag receiving a command with incorrect AuthMethod or Step fields shall respond either with an “insufficient privileges” or an “other error” error code. The crypto suite shall transit to the **Init** state.	M	Tag	By demonstration using Test Pattern 3 and Test Pattern 4
20	8.1	An Interrogator receiving a Tag’s response with incorrect AuthMethod or Step fields shall reset the Tag and try to restart the communication.	M	Interrogator	By design
21	8.2	All Authenticate commands for Tag identification shall use AuthMethod = 11b in accordance with 10.3.	M	Tag	By demonstration using Test Pattern 1 or Test Pattern 2
22	8.2.1	The crypto suite state transitions for Tag identification in partial result mode shall be as specified in Figure 4.	M	Interrogator, Tag	By design
23	8.2.2	The crypto suite state transitions for Tag identification in complete result mode shall be as specified in Figure 5.	M	Interrogator, Tag	By design
24	8.2.2	In case of failure during one of the steps of the protocol, the crypto suite transits to the **Init** state.	M	Tag	By design
25	10.1	The sequence of messages exchanged for Tag identification in partial result mode shall be as depicted in Figure 8.	M	Interrogator, Tag	By design
26	10.1	The sequence of messages exchanged for Tag identification in complete result mode shall be as depicted in Figure 9.	M	Interrogator, Tag	By design
27	10.1.1	In Step 1 of the partial result mode, the Interrogator message shall include a random challenge to request the Tag to send its identification data.	M	Interrogator	By design
28	10.1.1	Upon reception of this message, the Tag shall start calculating the response.	PRM	Tag	By design
29	10.1.1	The first response of the Tag shall be the total length of the identification cryptogram.	PRM	Tag	By design
30	10.1.1	In Step 2 of the partial result mode, the Interrogator shall retrieve the fragments of the Tag’s identification cryptogram by chaining further Authenticate commands and responses.	M	Interrogator	By design